# Lecture Notes in Computer Science 12812

More information about this subseries at http://www.springer.com/series/7410

Thomas Groß · Luca Viganò (Eds.)

# Socio-Technical Aspects in Security and Trust

## 10th International Workshop, STAST 2020
Virtual Event, September 14, 2020
Revised Selected Papers

Springer

*Editors*

Thomas Groß
Newcastle University
Newcastle upon Tyne, UK

Luca Viganò
King's College London
London, UK

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-030-79317-3 ISBN 978-3-030-79318-0 (eBook)
https://doi.org/10.1007/978-3-030-79318-0

LNCS Sublibrary: SL4 – Security and Cryptology

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

# Preface

The 10th International Workshop on Socio-Technical Aspects in Security (STAST 2020) aimed at creating an exchange of ideas and experiences on how to design systems that are secure in the real world where they interact with non-expert users. The term "socio-technical," in this context, means a reciprocal relationship between technology and people. The 2020 workshop focused especially on the interplay of technical, organizational, and human factors in achieving or breaking computer security, privacy, and trust.

As typical for STAST, the workshop received a wide range of inter-disciplinary submissions with a number of distinct methodologies - 11 submissions used quantitative methods, such as statistical inference, to make their argument, whereas 21 submissions employed qualitative methods, such as semi-structured interviews. We received five submissions in protocol design (with underpinning in cryptography or formal methods) and five submissions in security analysis (on vulnerabilities or attacks). Two submissions were review papers. Seven submissions focused on research methodology, that is, instrument evaluation, meta-research, or research synthesis.

The peer-review was organized as a double-blind process. Each submission received a minimum of three reviews. Submissions with appreciable variance in review scores were assigned a fourth review as a tiebreaker. On average, we had 3.2 reviews per submission. The peer-review process included an active discussion phase, facilitated by a designated discussion lead for each submission, who subsequently summarized the discussion outcome and agreed conclusions in a meta-review.

STAST benefited from a strong conflict-of-interest management system, allowing the chairs to submit papers themselves while ensuring that an other chair could govern the submission, maintaining a strict separation-of-duty policy.

Of the 42 papers initially submitted to the workshop, 35 papers were retained by the chairs for peer-review after an initial check against the stipulations of the call for papers. Eventually, we accepted 11 submissions for publication in this volume, yielding an acceptance rate of 31%, not counting the chairs' desk rejections.

We prepared this volume with the following sections. First, *Personality and Behavior* includes investigations on the impact of personality and traits on behavior. Second, *Behavior in Face of Adversaries* considers human behavior when confronted with a range of real-world attacks. Third, *Smart Environments* focuses on emergent smart systems, such as smart buildings and smart homes. Fourth, *Decentralized Systems and Digital Ledgers* includes analyses of decentralized systems, especially ledgers. Finally, *Reflections on Socio-Technical Aspects of Security* includes analyses of, and positions on, the past and future of the field itself.

Simon Parkin and Yi Ting Chua were recognized with the STAST 2020 Best Paper Award for their paper *Refining the Blunt Instruments of Cybersecurity: A Framework to Coordinate Prevention and Preservation of Behaviours.*

Overall, we are very pleased with the quality of STAST's 10th anniversary volume. We are grateful for the high-quality work of the authors involved and for the invaluable contributions of the 33 Program Committee members and 4 external reviewers, whose dedication and attention to details enabled this volume.

December 2020

Thomas Groß
Luca Viganò

# Message from the Workshop Organizers

It has been ten years since we had the idea of founding a workshop dedicated to socio-technical aspects of cyber-security. At that time, something was missing in the landscape of events in security research: a venue in which to discuss security in a broader manner, a manner that combined technical discussion with other topics traditionally linked to usability and human computer interaction research, yet much broader than just these. There was a need to discuss attacks that exploit technical hacking in combination with social engineering and, equally, there was a need to discuss user practices, organizational processes, and social culture as instruments to establish security or, by contrast, as possible vectors to break it.

Discussing such matters was, and still is, relevant since evidence shows that designing systems that are secure when analyzed from a merely technical perspective, regardless of the values and merits of the approach, does not guarantee that security works as expected once deployed. The common and arguable explanation is that the human, the "weakest link," did not comply. However, blaming users neither helps nor gives us instruments to design stronger systems. We have learned by experience that a better strategy is to holistically conceive systems whose security emerges by harmonizing the technical features with the modalities in which humans, organizations, and societies operate. The manifesto of addressing security problems socio-technically means exactly that all the components are addressed as a whole. We have also learned that such a manifesto has a very wide impact, encompassing virtually all application areas where human beings may play a role in the effectiveness of security measures; hence, it concerns virtually every ICT application that must be protected from criminals.

Looking at the proceedings of this year's edition of the workshop, the published contents clearly attest that the idea outlined above has rooted well. As a result, the International Workshop on Socio-Technical Aspects in Security (STAST) is now fully mature. Its aims have come to a clear focus, and the affiliation with the European Symposium on Research in Computer Security (ESORICS) is naturally well principled and practically fruitful.

We would like to thank all the Program Chairs and Program Committee members who over the last decade have helped STAST become a successful event. And we are particularly grateful to this year's Program Chairs, Thomas Groß and Luca Viganò: they have done an impeccable job and brought, with a top-level Program Committee, this year's edition to an unmatched success with a great scientific program.

December 2020

Giampaolo Bella
Gabriele Lenzini

# Organization

## General Chairs

| | |
|---|---|
| Giampolo Bella | University of Catania, Italy |
| Gabriele Lenzini | University of Luxembourg, Luxembourg |

## Program Committee Chairs

| | |
|---|---|
| Thomas Groß | Newcastle University, UK |
| Luca Viganò | King's College London, UK |

## Programme Committee

| | |
|---|---|
| Luca Allodi | Eindhoven University of Technology, Netherlands |
| Kalliopi Anastasopoulou | University of Bristol, UK |
| Panagiotis Andriotis | University of the West of England, UK |
| Ingolf Becker | University College London, UK |
| Giampaolo Bella | University of Catania, Italy |
| Zinaida Benenson | University of Erlangen-Nuremberg, Germany |
| Tobias Blanke | University of Amsterdam, Netherlands |
| Michael Carter | Queen's University Belfast, UK |
| Lynne Coventry | Northumbria University, UK |
| Sarah Diesburg | University of Northern Iowa, USA |
| Verena Distler | University of Luxembourg, Luxembourg |
| Lothar Fritsch | Karlstad University, Sweden |
| Rosario Giustolisi | IT University of Copenhagen, Netherlands |
| Thomas Groß | Newcastle University, UK |
| Pieter Hartel | University of Twente, Netherlands |
| Ulrike Hugl | Innsbruck University, Austria |
| Markus Jakobsson | ZapFraud, USA |
| Kat Krol | Google, UK |
| Shujun Li | University of Kent, UK |
| Jean Martina | Universidade Federal de Santa Catarina, Brazil |
| Maryam Mehrnezhad | Newcastle University, UK |
| Masakatsu Nishigaki | Shizuoka University, Japan |
| Jason Nurse | University of Kent, UK |
| Simon Parkin | University College London, UK |
| Saša Radomirovic | University of Dundee, UK |
| Karen Renaud | Abertay University, UK |
| Peter Y. A. Ryan | University of Luxembourg, Luxembourg |
| Diego Sempreboni | King's College London, UK |

| | |
|---|---|
| Kerry-Lynn Thomson | Nelson Mandela Metropolitan University, South Africa |
| Theo Tryfonas | University of Bristol, UK |
| Luca Viganò | King's College London, UK |
| Konrad Wrona | NCI Agency/Military University of Technology in Warsaw, Poland |

## Additional Reviewers

Susanne Barth
Lucas Palma
Borce Stojkovski
Samuel Wairimu

## Publicity and Web Site Chairs

| | |
|---|---|
| Borce Stojkovski | University of Luxembourg, Luxembourg |
| Itzel Vazquez Sandoval | University of Luxembourg, Luxembourg |

## Sponsors

Fonds National de la Recherche Luxembourg

SnT
securityandtrust.lu

UNIVERSITÀ degli STUDI di CATANIA

uni.lu
UNIVERSITÉ DU LUXEMBOURG

# Contents

## Personality and Behavior

## Behavior in Face of Adversaries

## Smart Environments

## Decentralized Systems and Digital Ledgers

## Reflections on Socio-Technical Aspects of Security